Design and Proposal of an Implementation method for Unauthorized Access Tracing System

DR. M. THANGAVEL, M.C.A., M.PHIL., PHD, A. ARONI AMALA KARTHIKA, M. MATHIVATHANI
HEAD OF THE DEPARTMENT , MCA III, MCA III
ERODE SENGUNTHAR ENGINEERING COLLEGE
THUDUPATHI

ABSTRACT—At present, the number of unauthorized access incidents on the internet is growing, and the current access control technologies cannot stop specific way of access. We had proposed a hop-by-hop IP traceback method that can reliably trace a source of an attack. In this paper, we describe the development and the evaluation of our prototype system. The main features of our proposed method are the packet feature, which is composed of specific packet information contained in a packet for identification of an unauthorized packet, and the algorithm using datalink identifier to identify a routing of a packet. We show the development of the prototype system equipped with our tracing functions on routers and its processing result. We here adopt a distributed management approach that controls the tracing process and information within a particular group of networks. Implementation of Tracer

1. packet conversion and store process
2. trace and search process

trace and search process has two modules: packet search module and upstream network interface decision module

INTRODUCTION

While the Internet as a business infrastructure increases its importance, the number of unauthorized access incidents on the Internet is growing, and such activity tends to cause a great problem. At present, the access control technologies including firewalls are commonly used to prevent unauthorized access, but some specific way of access cannot be stopped by the access control technologies. Nowadays installing Intrusion Detection Systems (IDS) coupled with firewalls, and monitoring networks enables us to quickly detect and react to The ability required to perform traceback is “to identify the true IP address of the terminal originating attack packets.” If we can identify the true IP address of the attacker’s terminal, we can also get information about the organization (e.g. name or telephone number) involved in the attack or the attacking terminal. As the method of the source pursuit of unauthorized access, some researches using IP (Internet Protocol) are performed. The source pursuit using IP is called IP Traceback. Unauthorized access. Figure (a) shows a current dealing with unauthorized access. However, even if these tools can detect unauthorized activities, their sources cannot be identified. The reason is that denial of service (DoS) attacks, which have recently increased in number, can easily hide their sources and forge their IP addresses. Thus, it is not possible for the access control alone to be a factor...
of unauthorized access. As the measure of unauthorized access, it is necessary to pinpoint the source in order to prevent the unauthorized activity. For this reason, we have been studying a method to identify the source of an authorized activity and developed a prototype system. IP traceback methods can be divided into two groups.

**Proactive tracing:**

This prepares information for tracing when packets are in transit. In a case where packet tracing is required, the target of the attack refers information and identifies the source of the packets.

**Reactive Tracing:**

This “reactive tracing” starts tracing when required. In our study, we have selected reactive tracing that does not increase network traffic at normal times and generates traffic for tracing only when actual tracing is required.

**The Trend of the Reactive Tracing Methods:**

![Figure (b) Hop-by-Hop Tracing](image)

The majority of reactive tracing methods trace the attack path from the target back to the source. The challenges involved in this type of method are traceback algorithm and packet matching technique.

1. **Hop-by-Hop Tracing**

   This method is to trace an IPsec identifies the travel path and the source of packet from the target back to the source hop-by-hop. Since this technique uses existing hop, and trace the source based on the incoming IPsec protocol, it has an advantage that it is not packets that arrive one after another during a flood necessary to implement a new protocol. type attack. Figure (b) shows a flow of trace to detect the source hop-by-hop.

2. **Hop-by-Hop Tracing with Overlay Network**

   Patterns observed at the entry and exit point of the particular problems involved network based on the network map. in tracing routers hop-by-hop are
that if there are Traceback Approaches too many hops, the number of necessary. In the field of reactive tracing study processing for tracing will be increased. As then several methods that identify a source of a packet result, it will take a longer time to trace, and with forged source IP address have been information for tracing can be lost before trace proposed. Although most of the existing processing is completed. Therefore, a method to techniques deal with flood type DoS attacks, there build the overlay network for tracing purposes that are more attacks using only one or a few IP involves a less number of hops is proposed. With packets such as attacks exploiting IP fragment. It this method, IP tunnels between the edge routers is important to be able to trace unauthorized and the special tracking routers are created, and access using single packet. the IP packets are rerouted to the tracking router. Based on the above, we have proposed a via IP tunnel. Hop-by-hop tracing is performed hop-by-hop traceback method. We are developing over the overlay network that consists of IP a system implementing our method even if the tunnels and tracking routers attacker forges its source IP address. Our system

(3) IPsec Authentication

performs real-time tracing and exactly identifies Another proposed technique is that when the source of the specific packet along the attack unauthorized access is detected, a Security path. association (SA) of the IPsec is created. Our Traceback Architecture

Traceback Method

In general, the source IP address of each unit or install a single manager as a central packet can easily be forged at the source of the manager of the entire network. packet. On the other hand, it is difficult for a sender of a packet to forge the datalink-level Basic model of our traceback method in identifier when sending packets, because, in the practical terms, particularly network policy may event of frame or cell transfer, forwarding unit restrict tracing a packet with certain limitation. (such as router) in turn converts the datalink-level We cannot trace a packet beyond our own identifier to the interface identifier of the unit. network perimeter if neighboring networks Therefore, at each forwarding unit, we can impose different policy. identify its adjacent unit having forwarded a We therefore adopt a distributed particular packet based on the datalink-level management approach that controls the tracing identifier of the adjacent unit and the datalink- process and information within a particular group level identifier corresponding to the packet. of networks. This control section is called as In our approach, forwarding nodes, or Autonomous Management Network (AMN). tracers, keep data about an incoming packet and The monitoring manager, which is its datalink-level identifier such as source MAC deployed in each AMN, executes a tracing process Address in a buffer memory address within its tracing process goes beyond the AMN’s corresponding to their datalink-level identifier in boundary, the monitoring manager of the AMN each forwarding unit and identify the adjacent unit that initiated the tracing process asks the by searching for the datalink-level identifier of the monitoring manager in the adjacent AMN to trace forwarded packet that corresponds to an attack packet.
**Process Flow:**

Beginning with the forwarding unit closest Our traceback approach involves several to the sensor that has detected unauthorized Steps, from attack detection to source access, we identify each adjacent forwarding unit identification, along the attack path, and ultimately reach.

**Step 1:** Sensors are deployed at each target source of the attack packet even if a forged source network. When a sensor detects an attack, it IP address is used.creates data containing features of the attack Our Traceback Modelpacket and sends a tracing request to the. In this section, we describe our trace back monitoring manager deployed in its AMN.
architecture that identifies the source of a packet

**Step 2:** The monitoring manager order the with forged source IP address. The architecture AMN’s tracer to trace the attack packet. The consists of the following three components: tracer identifies the adjacent node and returns.

**(1)Sensor**

This component is deployed at target site unauthorized access from the network another is to request a manager to start tracing.

**(2)Tracer**

This component implements a function in forwarding nodes to maintain information about forwarded IP packets as well as a function to trace packet along the attack path on forwarding unit.

**(3)Monitoring Manager**

In response to a request from a sensor, this component controls tracers and manages the entire tracing process.
**Step 3:** Based on the result returned, the process described above continues until the tracer identifies the attack packet’s source.

**Step 4:** If a tracing process goes beyond the AMN’s boundary, processing is handed over to the relevant monitoring manager that controls that AMN.

**Step 5:** The monitoring managers in each AMN traces the packet in their AMN and sends the tracing result to the monitoring manager that initiated the traceback request.

**Step 6:** The requester monitoring manager sends the final results to the sensor that requested the trace.

- A part of IP data If we create a packet feature consisting of only IP header fields, identical packets may exist. Therefore, in order to improve the precision of packet identification, we decide to include a part

<table>
<thead>
<tr>
<th>0</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Header Length</td>
<td>Type of Service Identification</td>
<td>TTL</td>
<td>Protocol</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>Destination IP Address</td>
<td>Options</td>
<td>Padding</td>
<td></td>
</tr>
</tbody>
</table>

**IP Data Part —— MAX( 20 Bytes)**

**Structure of Packet Feature**
Implementation of Our Traceback System

We have developed a traceback system based on our architecture and protocol. Implementation Model

Packet Feature

Our traceback method uses a packet feature as a parameter for Trace Request and Trace Order. In order to uniquely identify the individual packet, we extract several fields of the IP packet that are not altered by tracers and create a packet feature. The extracted fields are as follows:

- Version
- Header Length
- Identification
- Protocol
- Source and Destination IP addresses

of IP data field (maximum 20 bytes). The following figure shows the structure of the packet feature.

31Total Length Flags Fragment Header Checksums On our traceback method, we implement sensor for detecting unauthorized access and for making a trace request, tracers for executing trace

Trace Algorithm

We have developed the algorithm that processes Trace Order reception, trace execution for upstream path decision and trace report. Below we describe our algorithm.

Step 1: Start the Tracing process.

Step 2: Receive the packet feature and passed it to packet search module.

Step 3: Check Packet Information Area with packet feature received.

Step 4: If any match found then let matched record as target record.

Step 5: Compares the Address Information (i.e. MAC address) in target record with the address Information (i.e. MAC address & IP address) of the connected tracer stored in trace information.

Step 6: If match found decide IP address and return to the monitoring manager as trace result.

Step 7: Repeat step 3 to step 6 until source of the attack is detected.

Step 8: Stop the Tracing Process.

Information Management

There are two types of information used in tracers. One is the packet information that converts traversed packets information into packet features and stores them, and the other is the network interface information that stores network interface information between two units connected each other.

(1) Packet Information Area
Packet Information Area contains packet features which includes network interface information and forwarding time of the packet necessary information for tracing. On our implementation, records are stored in the memory area of the tracer for the purpose of real-time processing. If the volume of Packet Information Area exceeds the memory capacity, the oldest record will be deleted and the latest one will be stored in turn.

(2) Trace Information

We have studied three methods for obtaining network interface information from the unit connected with the tracer.

Method 1: Trace table method

Checking the network interface number, IP addresses and physical addresses (e.g. MAC address on LAN) of the connected tracers in advance, and storing them in the unit.

Method 2: ARP table method

Using the ARP table stored in the unit to look up the IP address and physical address of the connected tracer when Trace Order is received.

Method 3: Order-driven query method

Without providing a fixed table, obtaining network interface information using the lower layer protocols (e.g. RARP protocol) in response to Trace Order. We have reviewed each method and reached the following conclusion: As network interface information is temporarily stored in the ARP table, some information may be changed when searching the table; Although the order-driven query method is suitable for obtaining the latest network interface information, the process is complicated and takes longer time because the query task to the adjacent node is called every time a trace order is issued. Therefore, we select the trace table method that provides real-time, reliable, and efficient tracing.

Conclusions and Future Work

We have created a traceback system that can pursue the source even if an IP address is forged, and have demonstrated the effectiveness of the traceback processing. We will consider the relationship among the network load, and the number of tracers. In the viewpoint of the introduction of the traceback, we have 2 subjects. rst subject is method to identify matching packets and identify the sources under DOS attack where identical packets are sent from different sources. Second subject is method to introduce the tracer function. At the first step, the introduction of this method assumes the limited network such as Intranet. We think that it is possible to implement the tracer function on all the network equipments in such a network environment. However, it is assumed that it is impossible to implement the tracer on all the network environments by the open network. Then, the method that the source can be pursued is needed when the tracer function is partially introduced. We will further study how to improve the accuracy of the packet search process and develop the IP.